Encentuate® Identity and Access Management (IAM)

Remote Access Integration Guide

Product version 3.6

Document version 3.6.3

Copyright notice

Trademarks

Contact information

For more information about this product or any support enquiries, contact us:

To log a support incident: https://customercare.encentuate.com

To reach us by phone:

- Americas: +1-800-ENCENTUATE ext 5 (+1-866-362-3688 ext 5)
- Asia Pacific: +65-6862-7085

Email: customercare@encentuate.com

Table of Contents

About this Guide

Welcome to the Encentuate IAM® Remote Access Integration Guide.

Use this guide to configure, manage, and troubleshoot the different remote access integration solutions for Encentuate IAM.

Purpose

This guide provides procedures to help configure and maintain the remote access integration solutions against Encentuate IAM.

Audience

The target users for this integration guide are highly technical users that can understand how an Encentuate product can be enhanced and customized for remote access purposes.

What's in this guide

The IAM Remote Access Integration solution provides an overview of the IAM Remote Access Integration's features and architecture.

Deployment and Installation lists the steps in the IAM Remote Access Integration deployment, the supported software versions, browsers, second factors, platforms, and network requirements. It also details the IMS Server installation steps; AD configuration wizard; and AccessAssistant, and Web Workplace installation.

Deployment Procedures lists the steps and describes the parameters in configuring the following: Encentuate Mobile Active Code settings, message connector for sending MAC, enabling MAC for applications and users, enabling RADIUS using the IMS Configuration Utility, AccessAgent for Terminal Services or Citrix settings, application links to embed in an enterprise portal, steps in configuring Aventail SSL VPN.

Document conventions

Refer to this section to understand the distinctions of formatted content in this guide.

Main interface elements

The following are highlighted in bold text in the guide: dialog boxes, tabs, panels, fields, check boxes, radio buttons, fields, buttons, folder names, policy IDs/names, and keys. Examples are: **OK**, **Options** tab, and **Account Name** field.

Navigation

All content that helps users navigate around an interface is italicized (for example: *Start >> Run >> All Programs*)

Cross-references

Cross-references refer you to other topics in the guide that may provide additional information or reference. Cross-references are highlighted in green and display the referring topic's name (for example: Document conventions).

Hyperlinks

Hyperlinks refer you to external documents or web pages that may provide additional information or reference. Hyperlinks are highlighted in blue and display the actual location of the external document or web page (for example: http://www.encentuate.com).

Scripts, commands, and code

Scripts, commands, or codes are those entered within the system itself for configuration or setup purposes, and are usually formatted in a Courier font.

For example:

```
<script language="JavaScript">

<!--

  ht_basename = "index.php";

  ht_dirbase = "";

  ht_dirpath = ""/" + ht_dirbase;

//-->

</script>
```

Tips or Hints

Tips or hints help explain useful information that would help perform certain tasks better.

Warnings

Warnings highlight critical information that would affect the main functionalities of the system or any data-related issues.

Acronyms

The acronyms used in this guide are listed below:

Acronym	Description
AD	Active Directory
FQDN	Fully Qualified Domain Name
GINA	Graphical Identification and Authentication
GSM	Global System for Mobile communication
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
IMS	Encentuate IMS Server
IP	Internet Protocol
IVR	Interactive Voice Response
JVM	Java Virtual Machine
MAC	Mobile ActiveCode
OATH	Initiative for Open Authentication
OTP	One-Time Password
PC	Personal Computer
PDA	Personal Digital Assistant
RADIUS	Remote Authentication Dial-In User Service
SMS	Short Message Service
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

About IAM Remote Access Integration

This chapter provides details on how the IAM Remote Access Integration is used for secure remote access and its main features. It also includes an architectural overview, and its deployment configuration.

This chapter covers the following topics:

System overview

It is common practice to have employees working from home offices, customer locations, and other remote sites. Modern organizations want to provide remote access to business-critical information for authorized users—anywhere, anytime—while retaining the highest levels of network security.

While industry experts advocate two-factor authentication to enhance remote access security, many companies have been put off by the complexity of implementation and the cost of administration.

The IAM Remote Access Integration provides the following benefits:

- **Easy to use:** Users can leverage existing devices like smartphones, PDAs, or pagers to ensure two-factor authentication and secure remote access to corporate networks over SSL VPN appliance.
- **No extra tokens to manage:** Users can leverage on their e-e-mail and personal mobile devices. No tokens to deploy, replace, or administer.
- **Convenience of multiple channels:** Users can choose to receive OTPs over a channel of their choice – mobile phone, e-e-mail, fax, or IVR.
- **Easy secure remote access from anywhere:** Users receive highly-secure transparent access to all network resources from any network environment or device.

- **Easy remote access control:** Managers can set-up and deploy a single secure access gateway for all users, internal and external, to all network resources with full control.

- **Security of one time passwords:** All one time passwords are generated upon successful verification of a user's identity. The passwords expire after a preset period or upon usage.

- **No installation of client software:** No need for client software to be installed.

- **Extensible, scalable solution:** Solution can be extended to support other identity and access management features such as single sign-on and user provisioning.

The IAM Remote Access Integration solution

The IAM Remote Access Integration provides easy, secure remote access anywhere, anytime. The solution delivers best-of-breed secure remote access from anywhere combined with two-factor authentication.

Users can access Web, desktop, and legacy applications using an SSL VPN appliance and ensure two-factor authentication through the use of a one-time Encentuate Mobile ActiveCode (MAC) password delivered to smartphones, PDAs, pagers, fax, or other mobile devices. Organizations can also leverage Encentuate IAM to provide single sign-on to applications that are accessible over the SSL VPN appliance.

Organizations can enable secure remote access for their mobile workforce with the highest levels of security, without the inconvenience and cost of implementing and administering separate authentication tokens. Users can leverage existing personal devices to secure access to corporate networks without requiring extensive training.

Organizations can also leverage Encentuate IAM to provide single sign-on to applications that are accessible over the SSL VPN appliance.

Architecture

The solution uses Encentuate Mobile ActiveCode to provide two-factor authentication to the SSL VPN appliance. For single sign-on to applications, the Encentuate AccessAgent for Terminal Services, Citrix, or Web Workplace can be used.

Encentuate Mobile Active Code

An Encentuate Mobile ActiveCode (MAC) is a one-time password that is randomly generated and event-based. MAC is generated on the IMS Server and delivered via a secure second channel such as text services (SMS) on mobile phones. It is used for strong authentication.

The solution provides two-factor authentication by delivering one-time passwords (OTPs) through SMS on mobile phones and other channels like pagers, e-e-mail, fax, and IVR systems. The central components of MAC are:

Encentuate IMS Server: The server provides centralized management of users and security polices. It provides the following capabilities:

- Centralized management and deprovisioning of users: The IMS Server allows administrators to manage users individually or by AD groups. The console can be used to revoke users and immediately deny access to corporate networks over the SSL VPN appliance.

- Secure one-time passwords: The passwords comply with FIPS 140-2 requirements.

- Consolidated user-centric logs for audit purposes: The solution provides comprehensive logs that can be used to generate custom audit reports for regulatory compliance requirements.

Encentuate Mobile ActiveCode Service Module: The Service Module determines if the user is authorized to remotely access the corporate network. The component is integrated with the IMS Server and generates ActiveCodes (OTPs) for authorized users.

Multiple Channels for receiving ActiveCode: The solution supports a variety of channels for receiving the OTP, including SMS on mobile phones and devices, pagers, e-e-mail, fax, and IVR systems. The user profiles and policies defined in the IMS Server govern the use of these channels.

Encentuate AccessAgent

This software manages user's identity, enabling sign-on/sign-off automation and authentication management. The following solutions are available:

- Encentuate AccessAgent for Windows: Operates on Windows-based client machines to provide sign-on/sign-off automation, authentication management, and session management.

- Encentuate AccessAgent for Terminal Services: Operates on Windows Terminal Server to provide sign-on/sign-off automation for applications running in Terminal Server sessions.

- **Encentuate AccessAgent for Citrix**: Operates on Citrix server to provide sign-on/sign-off automation for applications running in Citrix sessions.

- **Encentuate AccessAgent for Web Workplace**: Web portal that provides sign-on automation for Web applications without the need to install additional software on the client machine.

The AccessAgent manages an **Encentuate Wallet**—an identity wallet that stores a user's access credentials and related information (including user names, passwords, certificates, encryption keys).

Each user persona has an Encentuate Wallet that acts as a personal metadirectory. A lock protects each Wallet. The lock can be as simple as a password or some other authentication factor, or a combination. Use of the Wallet is governed by a set of identity wallet security policies.

SSL VPN appliance

Aventail, Juniper, and F5 SSL VPN are some of the appliances supported by the IAM Remote Access Integration.

These appliances provide seamless and secure user experience from managed or unmanaged devices when integrated with IAM Remote Access.

How the architecture works

The secure remote access solution supports the following typical use case: a user at a cybercafe tries to access enterprise resources from an unmanaged remote PC, where the user may not have Administrator rights to install any software.

❶ The user connects to SSL VPN using Web browser.

❷ The user enters AD user name and password.

❸ SSL VPN contacts IMS Server using RADIUS to verify credentials.

❹ The IMS Server sends MAC to user through mobile gateway or e-e-mail server.

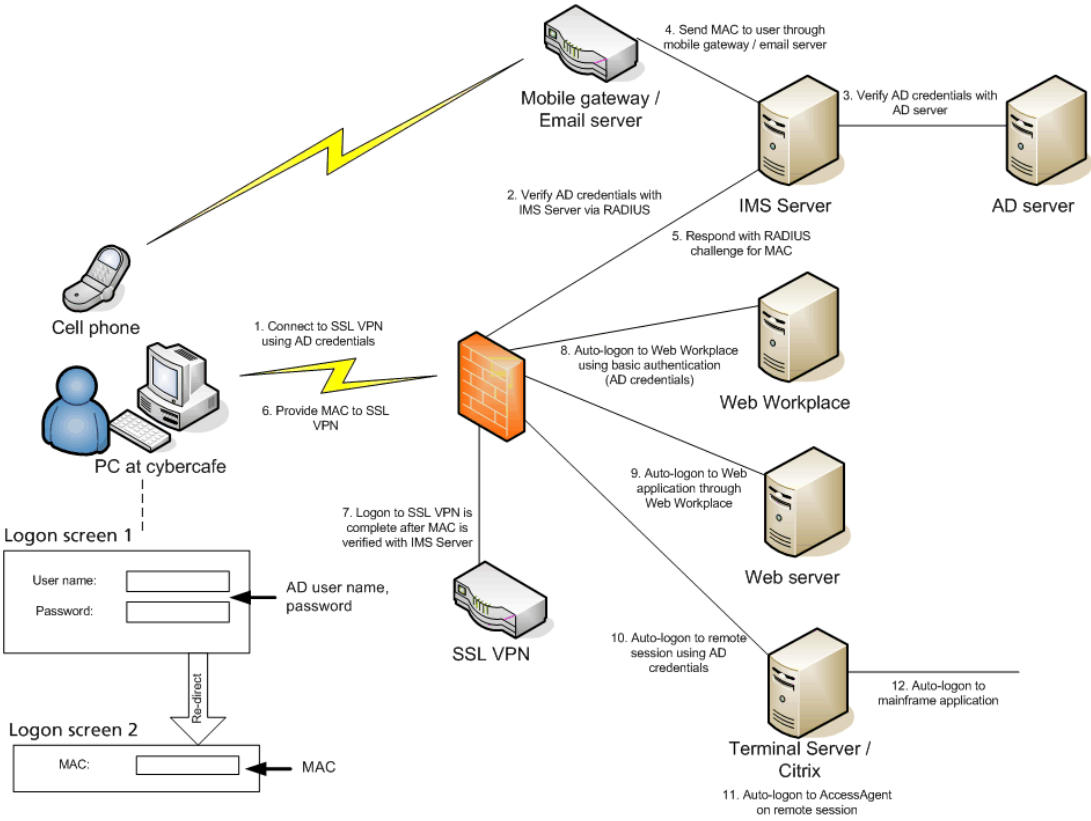
❺ The IMS Server also responds to SSL VPN with a RADIUS challenge.

❻ SSL VPN presents user with a prompt to enter the MAC.

❼ The user receives MAC and provides it to SSL VPN.

❽ SSL VPN verifies MAC with IMS Server. Upon successful verification, user is logged on to SSL VPN.

The architecture diagram describes the use cases.



Secure remote access solution architecture overview

After logging on to SSL VPN, user may be presented with a portal page that contains links to applications.

The following is a typical use case of what the user does after logging on to SSL VPN:

❶ The user clicks the link for a Web application.

❷ SSL VPN automatically logs on to Web Workplace using AD credentials.

❸ Web Workplace obtains application credentials from the user's Encentuate Wallet, and automatically logs on to Web application.

❹ The user clicks the link for a Terminal Server or Citrix server.

❺ SSL VPN launches graphical terminal agent that automatically logs on to Terminal Server or Citrix server using AD credentials.

❻ AccessAgent running in the Terminal Server's or Citrix server's remote session is automatically logged on using AD credentials.

❼ The user double-clicks on the icon of a mainframe application in the remote session's desktop.

❽ The mainframe application is launched and AccessAgent automatically logs on to it, using mainframe credentials stored in the user's Encentuate Wallet.

Deployment and Installation

This chapter covers the following topics:

Minimum system requirements

Supported software versions

- Aventail SSL VPN: 8.8 and above
- Juniper Networks Secure Access (SA) series of SSL VPN appliances, firmware version 5.4 and above
- F5 Networks FirePass series of SSL VPN appliances, firmware version 6.0 and above
- Encentuate IMS Server: 3.3.0.0 and above
- Encentuate Web Workplace: 3.3.0.4 and above
- Encentuate AccessAgent: 3.3.0.2 and above

Supported Web browsers

Any standard Web browser that supports JavaScript and cookies. The default configuration of these Web browsers are supported:

- Microsoft Internet Explorer 6.0 SP1 and above on Windows
- Mozilla Firefox 1.5 and above on Windows and Linux

To enable the use of SSL VPN appliance's graphical terminal agents for accessing Windows Terminal Services or Citrix, install and enable one of the following:

- ActiveX
- Sun JVM 1.4.2 plug-in
- Sun JVM 1.5.0 plug-in

Supported second factors

Any SMS or paging client, such as:

- Mobile phone
- Smartphone
- PDA
- Pager

Any e-e-mail client, such as:

- Mobile phone
- Smartphone
- PDA
- Web-based e-e-mail system

OTP tokens:

- Authenex A-Key OATH-only token (OATH-based OTP)
- VASCO Digipass GO 3 (time-based OTP)

Supported terminal service platforms

- Windows Terminal Services:
  - Windows 2000 Server
  - Windows 2003 Server
- Citrix:
  - Citrix MetaFrame XP FR2 and above
  - Citrix MetaFrame Presentation Server 3.0 and above

Network requirements

Only the following TCP ports need to be allowed through the enterprise firewall to the SSL VPN appliance:

- 80 (HTTP)
- 443 (HTTPS)

The ports for uploading and downloading are configurable.

Deploying the IAM RAI solution

To deploy the IAM RAI solution:

1. Install IMS Server for an integrated management system that provides a central point of secure identity management. For setup details, see Installing the IMS Server.
2. Install Web Workplace to manage the user's identity, and enable single sign-on to web-enabled applications across browsers, portals, and extranets. For setup details, see the Installing Web Workplace.
3. Configure an AD-based Enterprise Directory, with AD password synchronization enabled. For setup details see Installing the IMS Server.
4. Configure MAC settings at IMS Server. For setup details, see Configuring MAC settings in the IMS Server.
5. Configure message connector settings at IMS Server. For setup details, see Configuring a message connector.
6. Enable MAC settings for applications and users at IMS Server. For setup details, see Enabling MAC for applications and users.
7. Configure RADIUS interface at IMS Server. For setup details, see Configuring RADIUS interface at the IMS Server.
8. Configure SSL VPN appliance to direct authentication to the IMS Server and perform basic authentication to Web Workplace. For setup details, see Integrating with Aventail SSL VPN, Integrating with Juniper SSL VPN, Integrating with F5 SSL VPN.
9. Install AccessAgent on each Windows Terminal Server or Citrix server, if Windows Terminal Services or Citrix is used. For setup details, see Installing AccessAgent for Terminal Services or Citrix.
10. Embed links to applications, Windows Terminal Servers, and Citrix servers, in an enterprise portal as well. For setup details, see Embedding application links in an enterprise portal.

Details will be discussed in the succeeding sections.

Installing the IMS Server

Follow the instructions, depending on the type of installation you will be doing—new or an upgrade.

Installing Encentuate IMS Server

Before you install the IMS Server, ensure that you meet the following requirements:

- Windows XP, Windows 2000 Server, or Windows 2003 Server
- Monitor's resolution should be set to at least 256 colors
- Ports 80 and 443 are available

  Ensure that the following ports are not being used: 80 and 443

  If any of the ports are being used, free them by disabling the application that are using them. For example, Windows XP automatically starts Internet Information Server (IIS) on port 80. If you use Windows XP, you will need to disable IIS to make port 80 available.

- Encentuate IMS Server and Encentuate AccessAgent installation CDs.

Express installation

- If Microsoft SQL Server Express Edition/MSDE is already installed on this computer, you must have an Administrator (SA) account and password for Microsoft SQL Server instance.
- If Microsoft SQL Server Express Edition/MSDE is not already installed on this computer, you must have:
  - Microsoft Data Access Components (MDAC) 2.8 SP1 or above
  - Microsoft Windows Installer 3.1
  - Microsoft .NET Framework 2.0
  - Microsoft Windows 2000 SP4
  - Microsoft Windows XP SP2
  - Microsoft Windows 2003 SP1

Custom installation

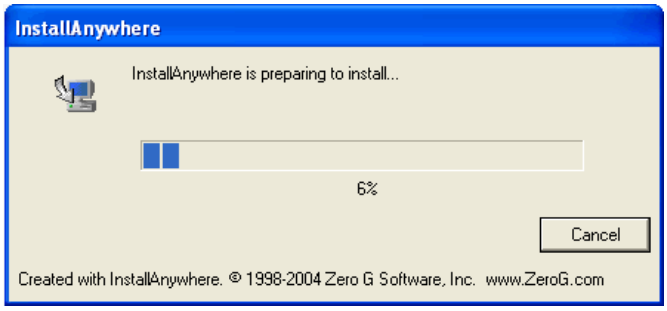
- For Microsoft SQL Server 2000:
  - Microsoft SQL Server 2000 (Standard, Enterprise or Desktop Edition) with Service Pack 3 and SQL Server Authentication enabled
  - Administrator (SA) account and password for Microsoft SQL Server
- For Microsoft SQL Server 2005:
  - Microsoft SQL Server 2005 (Standard, Enterprise or Express Edition) with Service Pack 1 and SQL Server Authentication enabled
  - Administrator (SA) account and password for Microsoft SQL Server
- For Oracle:
  - Oracle 9i/10g Database with an instance created for the Encentuate IMS Server
  - Administrator (DBA) account and password for this instance, to be used by the Encentuate IMS Server
- For installing database server locally:
  - Microsoft Data Access Components (MDAC) 2.8 SP1 or above
  - Microsoft Windows Installer 3.1
  - Microsoft .NET Framework 2.0

  Refer to Installing The IMS Database for more information.

Before installing the IMS Server, make sure your database and the SQL Server Agent have been started and that the SQL authentication is enabled.

To install the IMS Server:

1. Insert the Encentuate installation CD.
2. Go to *Start >> Run...*, click **Browse...**, and click **My Computer**. Right-click on the CD drive and select **Explore**.
3. Click on **imsinstall.exe** icon in the Encentuate installation CD.
4. InstallAnywhere extracts the installation files.

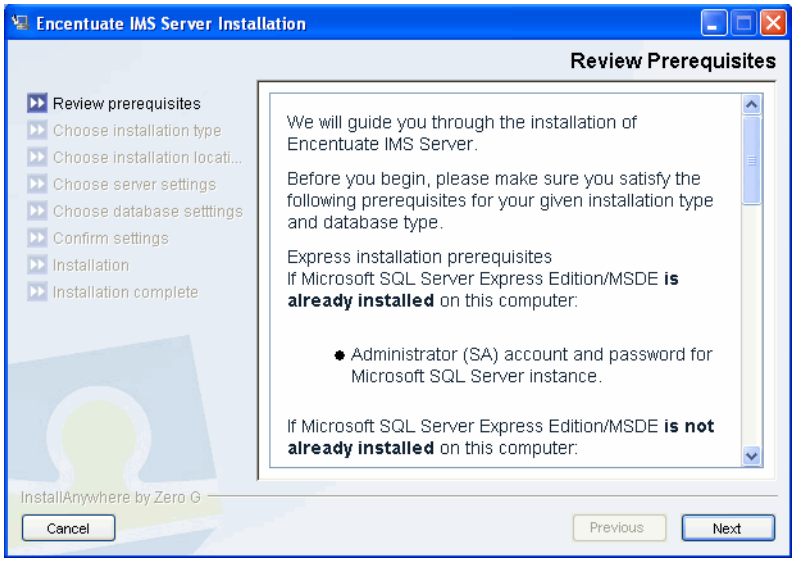


Extraction of installation files

5. The initial screen tells you to make sure you have the required setups, otherwise the installation will not proceed. Ensure you meet all the requirements before you continue.

   For more information on the requirements, see the Installation prerequisites in the IAM Administrator Guide.

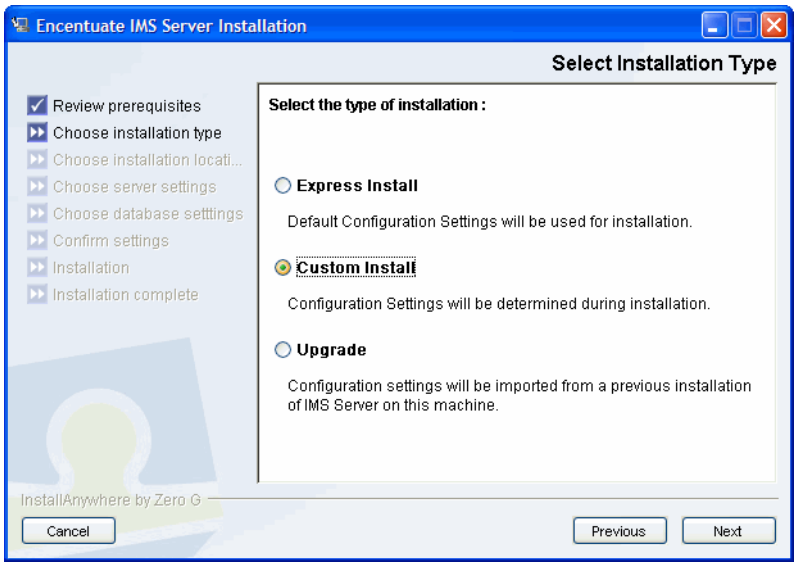
   Click **Next**.



Review prerequisites

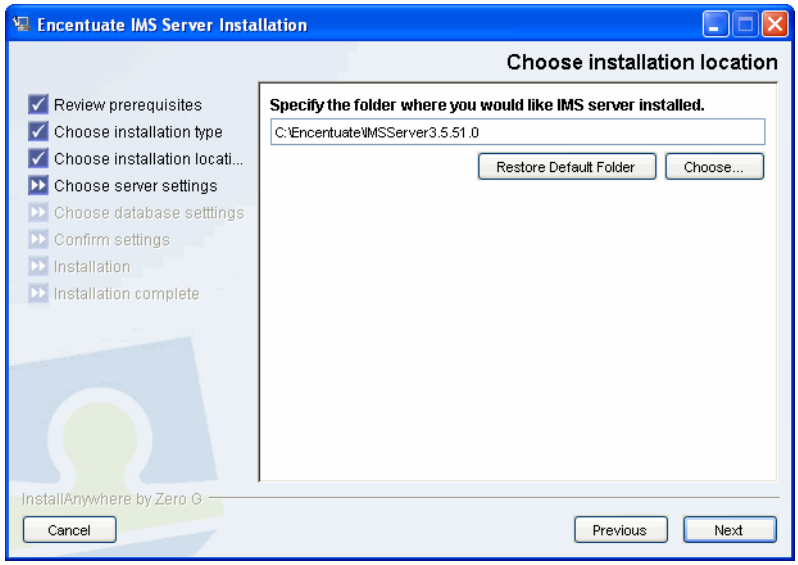
6. Select the installation type. Mark the **Custom Install** option. Click **Next**.

For this procedure, custom installation will be described.



Select installation type

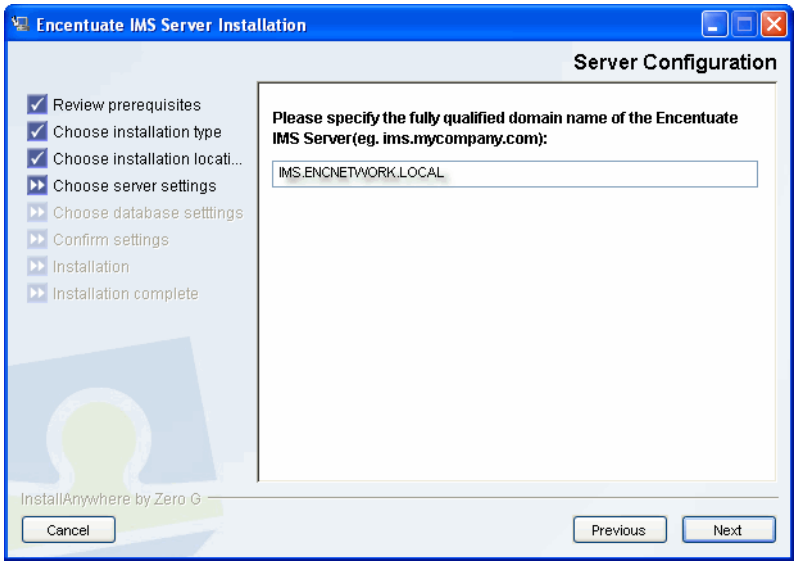
❼ Select the installation path where all the installation files will be stored. A recommended path containing the name and version of the IMS Server appears in the field.



Select installation path

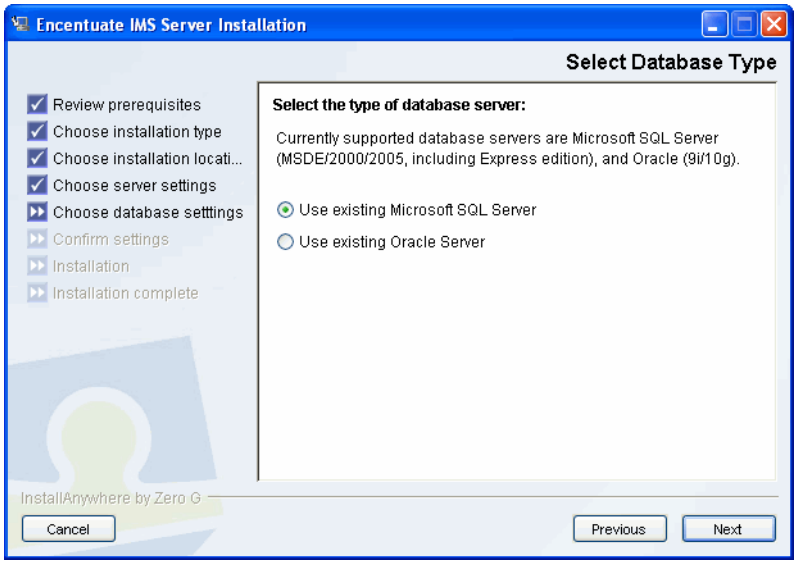
Click **Choose...** to customize the path and browse through your local hard drive. If you modify the path and revert to original recommended path later, click **Restore Default Folder**. Click **Next**.

8. Specify the hostname of the computer on which you are installing the Encentuate IMS Server. The hostname must be resolvable by all users. This is the same hostname that users must specify when they are installing AccessAgent and signing up a Wallet. Click **Next**.



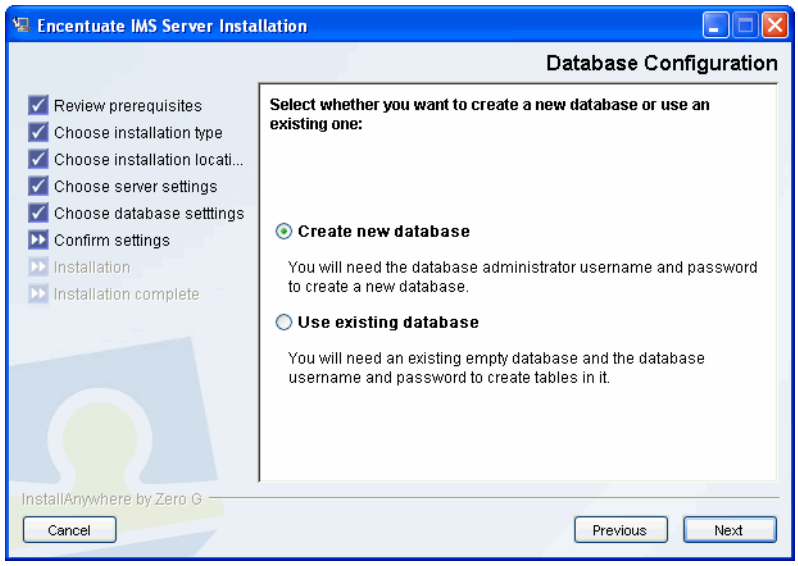
Specify IMS server hostname

9. Select the type of database to use for the system. Click **Next**.



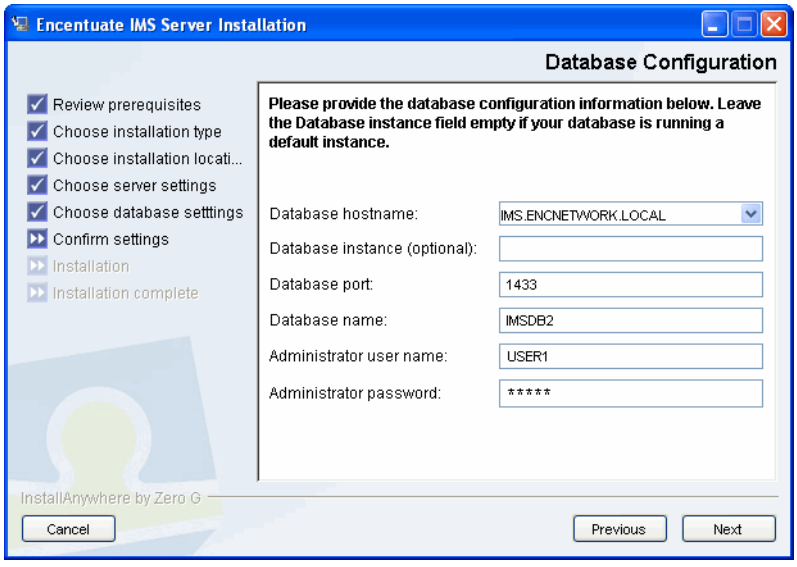
Select database type

❿ Specify whether you will create a new database or use an existing one.



Database configuration

⓫ In Database Configuration, specify the database host, port, and name. Enter your Administrator user name and password. Provide the name of the server where the database is located.



Database configuration

For MS SQL Server, the **Database Instance Name** may be left blank (indicating default). However, if you are using an Oracle database, you must specify the instance name.

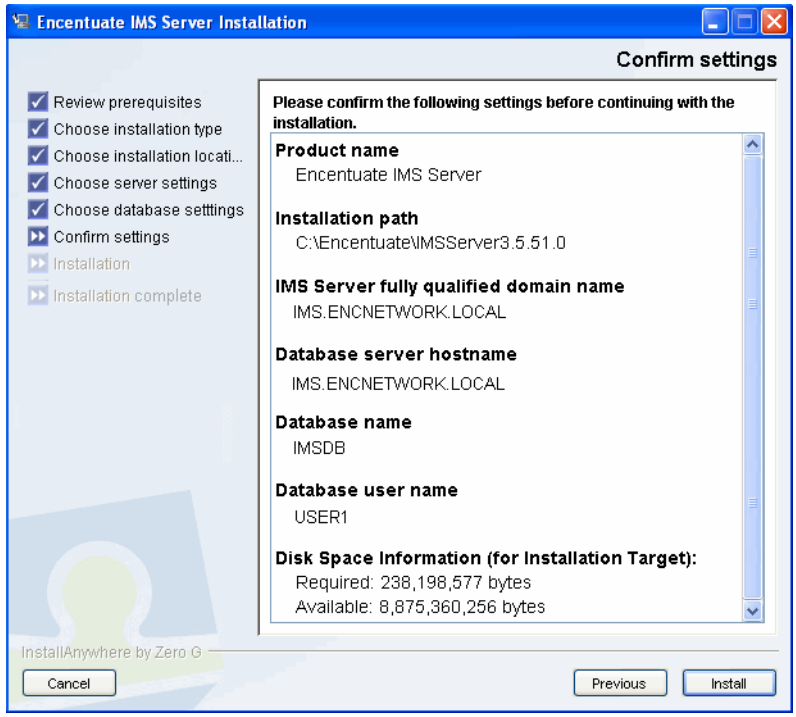
Enter the user name and password that will be used to connect to the database server.

Click **Next**.

The username and password entered must NOT be the database Administrator (Sa) account.

The installer checks if the database is ready. When connection settings are verified, the installation continues.

⓬ The Pre-Installation Summary window shows the details of your preferred configuration. Verify if all the settings are correct. To make changes before installing, click the **Previous** button.



Summary

⓭ Click **Install**.

After installation, the IMS Server uses the base connector for Encentuate user validation. The base connector enables any user to sign up as a new Encentuate user providing validation credentials.

To configure Active Directory, see Using the Setup Assistant (IMS Configuration Utility). Complete this task before making the IMS Server available to users for signup.

See the Authentication services section of the IAM Administrator Guide for more details.

Upgrading an existing installation of IMS Server

Refer to this procedure to import the configuration of a previous installation of Encentuate IMS Server.

For IMS Server upgrades, the existing settings (e.g., Java Virtual Machine, concurrent threads, etc.) are not affected. These settings are retained and do have to be reconfigured.

To upgrade the IMS Server:

1. Insert the Encentuate installation CD.
2. Go to *Start >> Run...*, click **Browse...**, and click **My Computer**. Right-click on the CD drive and select **Explore**.
3. Click on **imsinstall.exe** icon in the Encentuate installation CD.
4. InstallAnywhere extracts all the installation file.
5. Verify that you have the required setups, otherwise the installation will not proceed. To continue, click **Next**.
6. In the next window, select the type of installation to perform.
7. Choose **Upgrade**. Click **Next** and follow the succeeding instructions in the installation wizard.

Integrating with an enterprise's directory services

An enterprise can have numerous applications deployed on the enterprise network with perhaps as many directories to hold user accounts. This infrastructure makes it difficult to control audits, enforce policies, and de-provision at the enterprise level. All these are possible if the enterprise has a single point for collating user accounts.

An enterprise must identify which of the applications will be enterprise applications. Enterprise applications are specific to the business of an enterprise and controlled by an Administrator. Examples of enterprise applications are: Microsoft Windows, Lotus Notes, Active Directory, and other enterprise solutions such as SAP, PeopleSoft, Oracle, and Novell.

One of the enterprise applications will be used for enterprise identity binding. This is required to verify the identities of users who log on using Encentuate Keys. It also

allows for linking the IMS Server with the directory that the enterprise uses to manage their users. Refer to Enterprise identity in the IAM Administrator Guide for more information on enterprise identity binding.

For example, an enterprise has identified Active Directory for enterprise identity binding, as all user account information is stored in Active Directory.

When users register their USB Keys for the first time, they enter their user names and passwords for Windows. The IMS Server verifies the identities of users by checking with Active Directory. Once the server receives confirmation, the users can proceed with registration.

This is possible because certain configurations were made during the installation of the IMS Server allowing it to communicate with the enterprise's Active Directory.

Currently the IMS Server supports:

- Active Directory
- LDAP directories

Accessing the IMS Configuration Utility

After installing the IMS Server, the IMSService will automatically start and IMS Configuration Utility will open in your Web browser.

You can also click *Start >> Program Files >> Encentuate IMS Server >> IMS Configuration Utility* to open the IMS Configuration Utility. Select *Configuration Wizards >> Active Directory*. Select **Setup Assistant** to proceed with product activation. For more information, see Using the Setup Assistant (IMS Configuration Utility).

By default, the IMS Configuration Utility is installed on port 8080 and can only be accessed locally from the server console for security reasons (URL: http://imsserver:8080/).

You can also access the IMS Configuration utility using a Remote Desktop connection. Run the command: `mstsc /v imsserver`. When you are connected to the remote server, enter your Administrator user name and password to access the computer. Once connected, access the utility through the Windows Start menu.

Using the Setup Assistant (IMS Configuration Utility)

After installing the IMS Server, select **Setup assistant** from the IMS Configuration Utility navigation panel to configure your Active Directory.

If Active Directory is not the enterprise directory to be used, go to Basic Settings >> Enterprise Directories in the IMS Configuration Utility. In Enterprise Directories, click Add directory to add a new enterprise directory.

To use the setup assistant:

1. Select **Setup assistant** from the IMS Configuration Utility navigation panel. This displays the **Configure domains** start screen for the Active Directory configuration.

The **Configure domains** *screen will not be displayed if there is no domain configured in IMS. The user is taken directly to the* **Add domain** *screen instead.*

2. Configure the Active Directory.

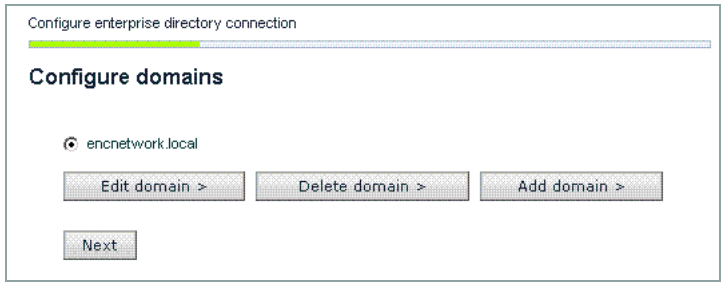
Configuring the Active Directory

You can configure your Active Directory as enterprise directory and assign valid domain user as Administrator in **Setup Assistant**.

To add a domain:

1. Select *Configuration Wizards >> Active Directory* from the IMS Configuration Utility navigation panel. This displays the **Configure Domains** screen.

   In the **Configure domains** screen, click **Add domain**.

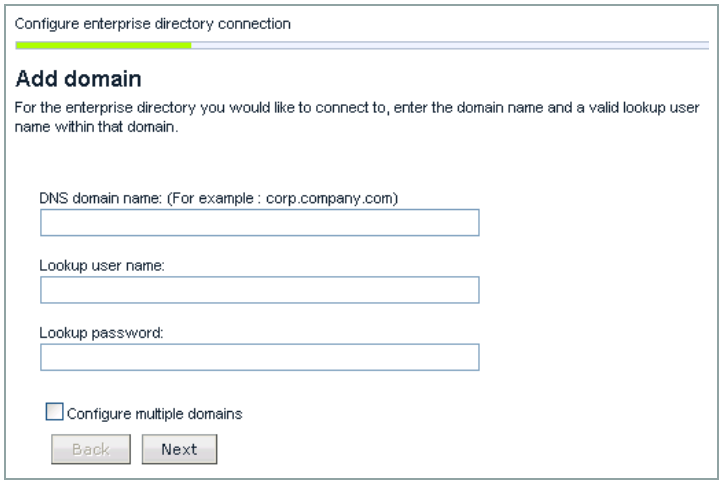


   The **Add domain** fields are displayed.

2. Enter information for the new domain.

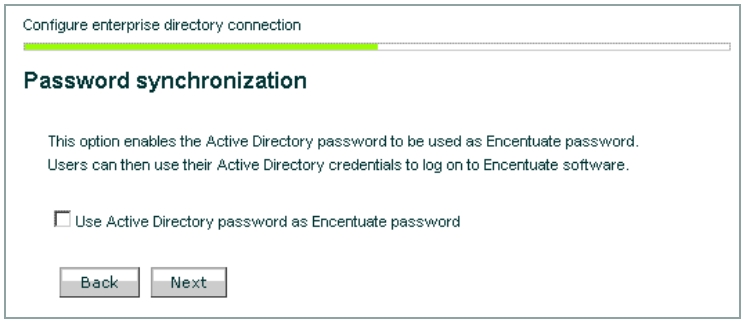
DNS domain name
Enter the DNS Domain Name for the Active Directory. This is usually of the form test.company.com.

Lookup user name
Lookup password
Enter the lookup user name and password. This is a valid domain user but does not have to have Administrator rights. These credentials will be stored on the IMS Server to facilitate validation of user credentials and searching for users and their attributes. The password for this account should be set such that it does not expire.



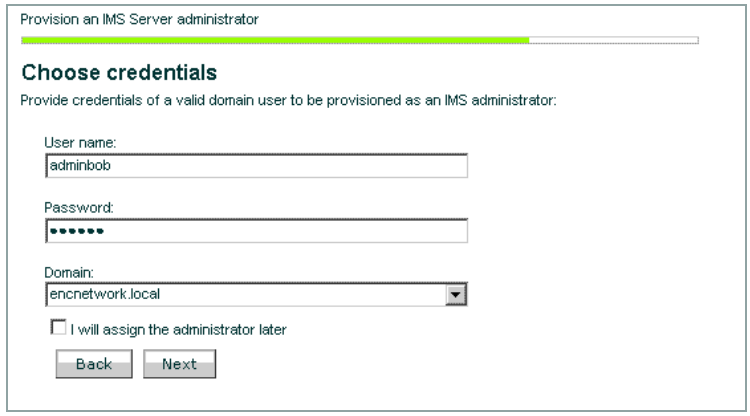
After completing all the fields, click **Next**. The **Password synchronization** screen is displayed.

❸ Selecting **Use Active Directory password as Encentuate password** will allow users to use their Active Directory password as their Encentuate password.



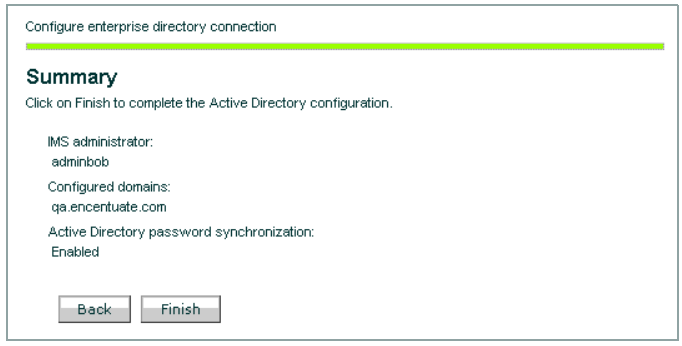
This is only useful if AccessAgent will be deployed. If this is a MAC-only deployment, this option can be left un-selected. Click **Next**. The **Choose credentials** screen is displayed.

❺ Enter the user name, password and domain of a valid Active Directory user. This user will be provisioned on the IMS Server and automatically promoted to Administrator role. If you would like to skip this step, select **I will assign the Administrator later**.

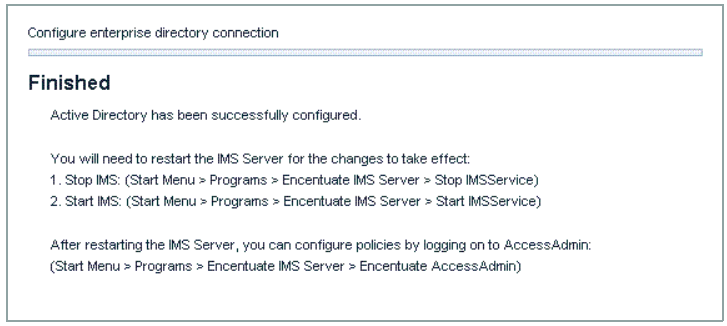


Click **Next**. The **Summary** screen is displayed.

❻ The screen shows a summary of the configuration settings. After reviewing the settings, click **Finish**.



If the configuration settings are applied successfully, another summary screen is displayed:



To modify an existing domain:

1. Select *Configuration Wizards >> Active Directory* from the IMS Configuration Utility navigation panel. The **Configure Domains screen** is displayed.
2. Select the existing domain and click **Edit Domain**.
3. Modify the values in the fields and click **Next** to apply changes.

To delete a domain:

1. Select *Configuration Wizards >> Active Directory* from the IMS Configuration Utility navigation panel. The **Configure Domains** screen is displayed.
2. Select the existing domain and click **Delete Domain**.

After making changes to the IMS Server using the Configuration Utility, restart IMSService for any changes to take effect.

To restart IMS Service, stop the IMSService (net stop IMSService), then start the IMSService (net start IMSService).

To start the IMSService, go to *Start >> Run* and enter **services.msc**. The Services window is displayed. Browse for IMSService then right-click and select **Start**.

Installing Web Workplace

There are two ways to install AccessAssistant and Web Workplace:

- with IMS
- without IMS

To install AccessAssistant and Web Workplace with IMS:

Install IMS Server (see Installing the IMS Server for details).

To install AccessAssistant and Web Workplace without IMS:

The following are in the installation package:

- WAR files: **AccessAssistant.war** and **WebWorkplace.war**
- **accessAnywhere.properties** file (in config folder).

  This is the configuration file for both AccessAssistant and WebWorkplace. The configuration key `WEB_WORKPLACE_ENABLED` needs to have the value "enabled" for Web Workplace.

Make sure that the IMS server name is also correctly set.

- **web_aa_sync_data.xml** file (in config folder): Default Web AccessProfiles.

  These AccessProfiles are already uploaded to IMS Server by default. However, if the IMS Server is upgraded from a previous version that does not contain these AccessProfiles, the file can be uploaded by using the "upldSync" IMS command-line tool: upldSync –-dataFile web_aa_sync_data.xml.

web_aa_sync_data.xml *contains AccessProfiles that can only be interpreted by WebWorkplace and not by AccessAgent.*

- **web_aa_sync_data_test.xml** (in config folder): Sample Web AccessProfiles.

  These AccessProfiles are not uploaded to IMS Server by default. The file can also be uploaded by using the "upldSync" IMS command-line tool: upldSync –-dataFile web_aa_sync_data_test.xml

- **canned_pages** folder: Folder containing default pre-stored logon forms (canned pages) for Web automatic sign-on.

WAR File installation

To deploy AccessAssistant or Web Workplace in the same Tomcat instance that the IMS Server is running in:

1. Stop the IMS Server.
2. Edit both **runserver.bat** in **<IMS Installation Folder>\ims\bin** folder and **installService.bat** in **<IMS Installation Folder>\ims\bin\installer** folder to include the system property: **accessAnywhere.configFile** specifies the location of the **accessAnywhere.properties** file.

   For example: set JAVA_OPTS=%JAVA_OPTS% -DaccessAnywhere.config-File=%CATALINA_HOME%\accessAnywhere.properties
3. In a command prompt, go to the **<IMS Installation Folder>\ims\bin\installer** folder and run `installService changeit` where `changeit` is the keystore password.
4. Copy the WAR file to **<IMS Installation Folder>**.
5. Start **IMS Server**.

An AccessAssistant or WebWorkplace folder should be automatically created within **<IMS Installation Folder>**.

For IMS Server versions lower than 3.5.0, the following must be done to auto-deploy the WAR file before starting the IMS Server:

1. Modify **server.xml** *in* **<IMS Installation Folder>\conf** *folder.*

2. Under the tag `<Engine Name="StandAlone" defaultHost="localhost" debug="0">`, *look for the* `"Host"` *tag and change the entries for unpackWARS, autoDeploy and liveDeploy to* `"true"` *as indicated:* `<Host name="localhost" debug="0" appBase="/" unpackWARs="true" autoDeploy="true" liveDeploy="true">`

Deployment Procedures

This chapter covers the following topics:

Configuring MAC settings in the IMS Server

The IMS Server must be configured to support either Password or MAC/OTP as the authentication service. Both authentication services cannot be supported at the same time.

To configure MAC settings in the IMS Server:

1. Run the IMS Configuration Utility (*Start >> All Programs >> Encentuate IMS Server >> IMS Configuration Utility*).
2. Under **Basic Settings**, select **ActiveCode Deployment** to open the panel.
3. Enter the mapping between the RADIUS client name and the MAC-enabled authentication service in the **NASID-application name binding** field.

The entry format should be: "RADIUS client name,authentication service ID".

For example (see Configuring RADIUS interface at the IMS Server): If the RADIUS client name is "AventailVPN" and the authentication service ID is "MAC", this entry should have the value "AventailVPN,MAC".

❹ Click **Add**.

❺ Select **true** or **false** from the **MAC-only registration of users** dropdown list to specify whether MAC-only user-registration is supported.

Set this to **true** *if you do not intend users to perform self-service sign-up through Web Workplace or AccessAgent.*

❻ Select **true** or **false** from the **Should Mobile ActiveCodes be sent out in upper-case?** dropdown list to determine whether MACs are sent out in uppercase or lowercase. MACs are not case-sensitive.

❼ Enter a search filter (name a value pair in a comma-separated list) in the **Search filter used for MAC-only registration of users UI** field.

This parameter specifies the comma-separated search filter used when users are searched on the User registration page.

For example: `sAMAccountName=*,objectClass=user`

❽ Specify the **Default messaging connector**. (see Configuring a message connector for details).

❾ Click **Update**.

Configuring a message connector

This section lists the parameters to configure for the message connector used in sending MACs. Use IMS Configuration Utility to do the setup.

The instructions below are for configuring a Web-based SMS Connector. Other types of message connectors are configured in the same way.

To configure a Web-based SMS Connector:

❶ Run the IMS Configuration Utility (*Start >> All Programs >> Encentuate IMS Server >> IMS Configuration Utility*).

❷ Under **Advanced Settings**, go to *Message Connectors >> Add Configuration Group*.

❸ Select **Web-based SMS Connector** from the dropdown list.

❹ Click **Configure**, and the **Web-based SMS Connector** panel is displayed.

❺ Enter a name for the message connector in the **Message Connector Name** field.

❻ Enter the identity attribute in the **Address Attribute Name** field. This will be used as the target address for sending messages.

For example: for an SMS message connector, the attribute can be “gsmNumber", which specifies the user’s phone number.

❼ Enter the GSM country code mapping to the corresponding SMS gateway IP address or hostname (for example, "65,127.0.0.1") in the **GSM code to gateway mappings** field.

Use this mapping if there are multiple SMS gateways handling different country codes. If there is only one SMS gateway, this setting can be left empty.

❽ In the **Default SMS gateway** field, enter the SMS gateway IP address or hostname to use if the current GSM code does not match any of the GSM codes to gateway mappings.

❾ Enter the name of the **Phone Number field** on the target web-form (on the SMS gateway) used to send the SMS.

❿ Enter the name of the **Message field** on the target web-form (on the SMS gateway) used to send the SMS.

⓫ Specify name-value mappings of the fields (for example, "group,executives") on the target web-form (on the SMS gateway) in the **Other fields**.

⓬ Under the **Advanced Configuration Keys** panel, in the **Fetch the address attribute from Enterprise Directory** field, specify whether the address attribute used by the messaging connector should be fetched from the Enterprise Directory.

Set to **false** if the address attribute (specified by "Address Attribute Name") is fetched from the IMS database.

Set to **true** if the performance will be degraded as each MAC issuance makes a call to the Enterprise Directory.

To support the fetching of multi-valued attributes (like "memberOf"), the ADSI connector should be used for configuring the Enterprise Directory (see the IAM Administrator Guide for details).

⓭ Enter the name of the attribute to be looked up from the Enterprise Directory (AD or LDAP server) in the **Enterprise directory address attribute** field.

This needs to be set only if **Fetch the address attribute from Enterprise Directory?** *is set to* **True**. *If this attribute specifies a phone number, it should be of the format "CountryCode-AreaCode-PhoneNumber" (for example: "1-650-4136800", "65--64735110").*

⓮ Specify the retry count value in the **HTTP retry count** field.

⓯ Specify the time-out value in the **HTTP timeout (milliseconds)** field.

⓰ Click **Add**.

Enabling MAC for applications and users

This section covers the following topics:

- Provisioning a user for MAC
- Enabling MAC

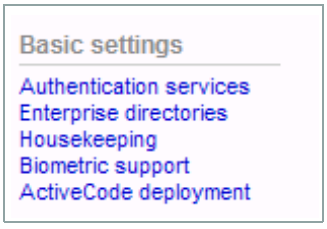
Provisioning a user for MAC

An Administrator or Helpdesk officer can register users to use MAC in AccessAdmin. Users can also perform self-service sign-up from Web Workplace.

To provision users for Mobile Active Code:

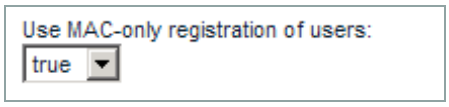
❶ Go to *Start >> Encentuate IMS Server >> IMS Configuration Utility*.

❷ Under **Basic Settings**, click **ActiveCode Deployment**.



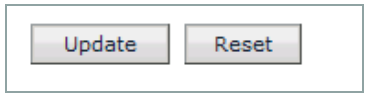
Click ActiveCode deployment

❸ Select **true** from the **MAC-only registration of users** field dropdown list.



Select true

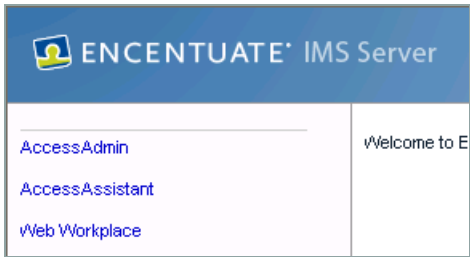
❹ Click **Update**.



Click the Update button

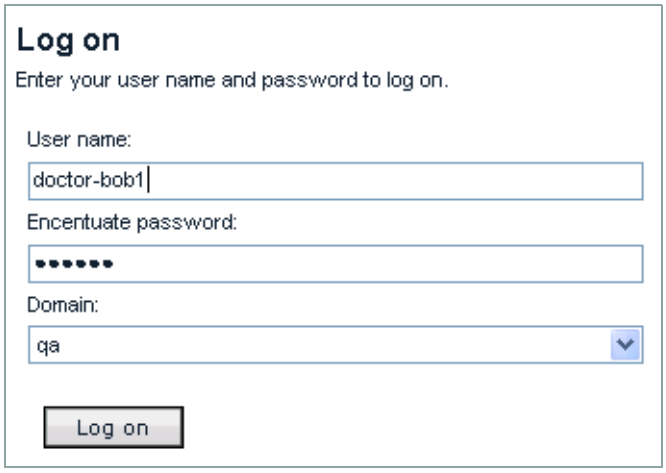
❺ Restart the IMS Server.

❻ Click **AccessAdmin**.



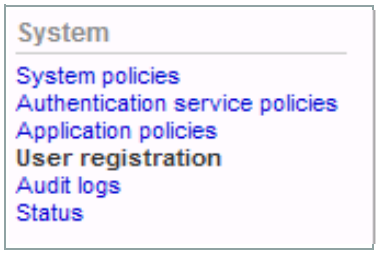
Click AccessAdmin link from the navigation panel

❼ Enter user credentials and click **Log on**.



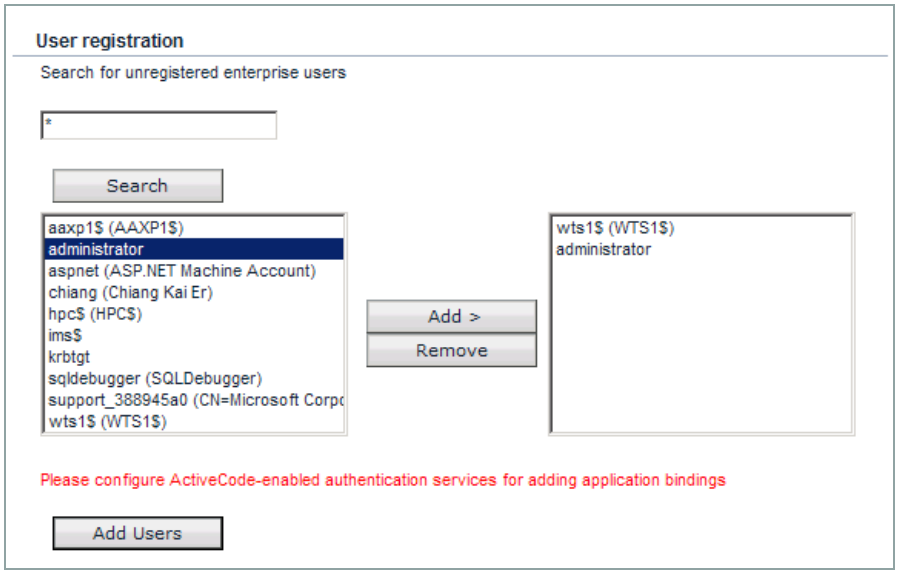
Click Log on

❽ Go to *System >> User Registration*.



Click the User registration link

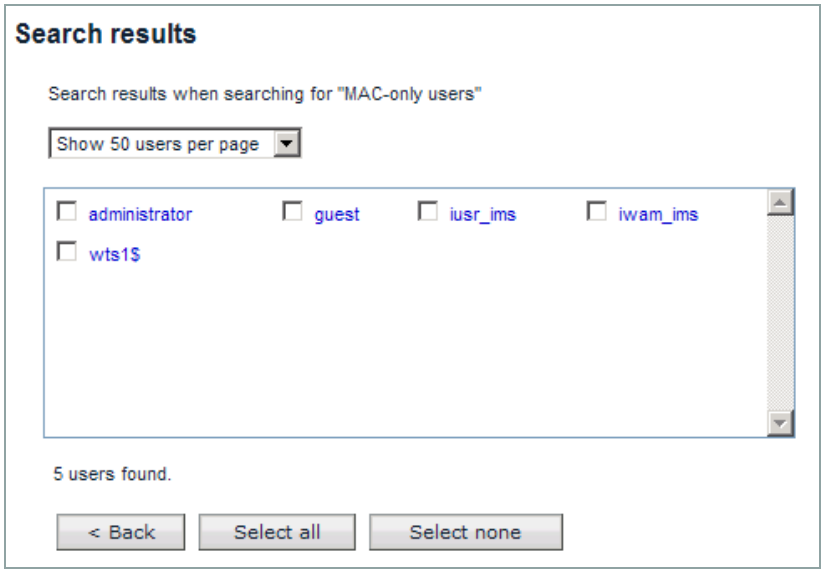
❾ Search for unregistered users in IMS.



Enter * and click Search to list all enterprise users

❿ Click **Add users**. A confirmation page is displayed.

A user who has been provisioned as a MAC-only user can only log on to the SSL VPN using an MAC. A MAC-only user cannot use either AccessAssistant and Web Workplace or AccessAgent. The user must sign up to either of the two applications to have access. See the Using Web Workplace and Signing up to AccessAgent in the IAM User Guide for details.



Click the link of the user name you are looking for

Enabling MAC

MAC can be enabled for two applications:

- SSL VPN (in this case, Aventail SSL VPN), or;
- AccessAssistant and Web Workplace

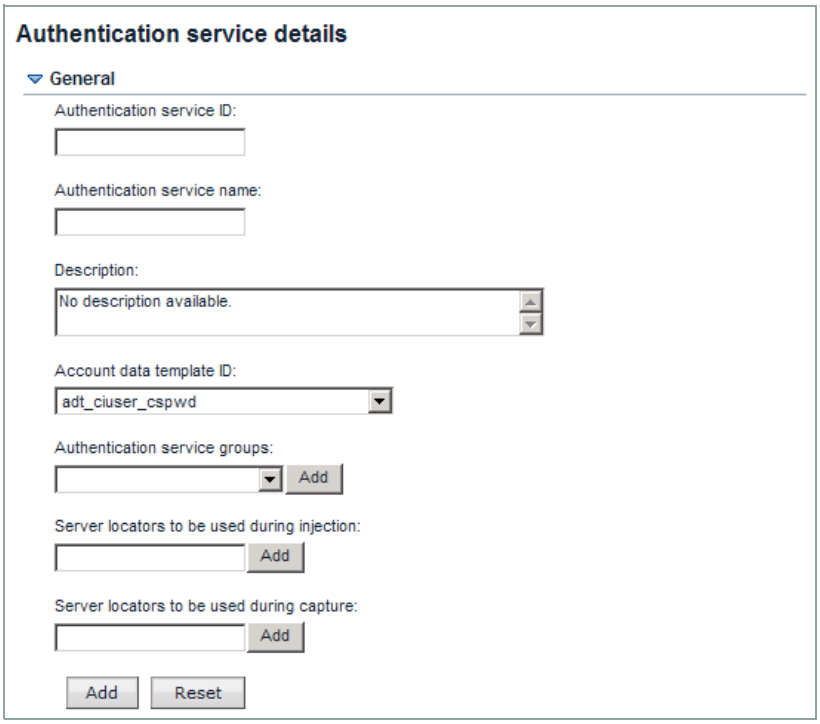
Enabling MAC for SSL VPN

To enable MAC for SSL VPN:

❶ Set up using IMS Configuration Utility.

To add a new authentication service for the MAC-enabled SSL VPN:

1. In the IMS Configuration Utility, add a new Authentication Service (*Basic Settings >> Authentication Services*).
2. Select **AccessAssistant** from the **Authentication Services** dropdown list. Click **Add new service**.



Add Authentication Services

3. Enter an **Authentication Service ID**. The ID will appear in the list of Authentication Services already created in the IMS Server.

4. Enter an **Authentication Service Name**. This name is visible to the user.

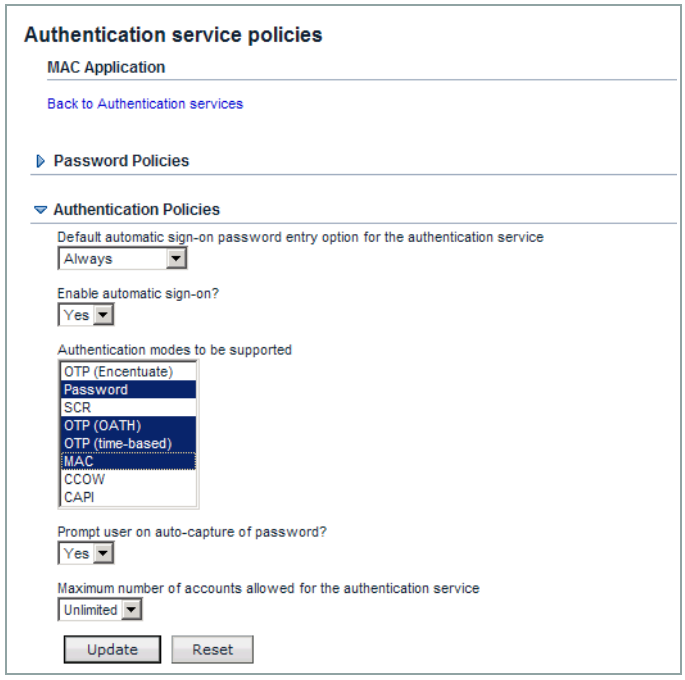
5. Click **Add** to save the configuration.

❷ Set up using Encentuate AccessAdmin

To set policies using AccessAdmin:

1. In the AccessAdmin navigation panel, go to *System >> Authentication Service Policies*.

2. Click the appropriate authentication service to change the authentication mode.



Authentication Services Policies panel

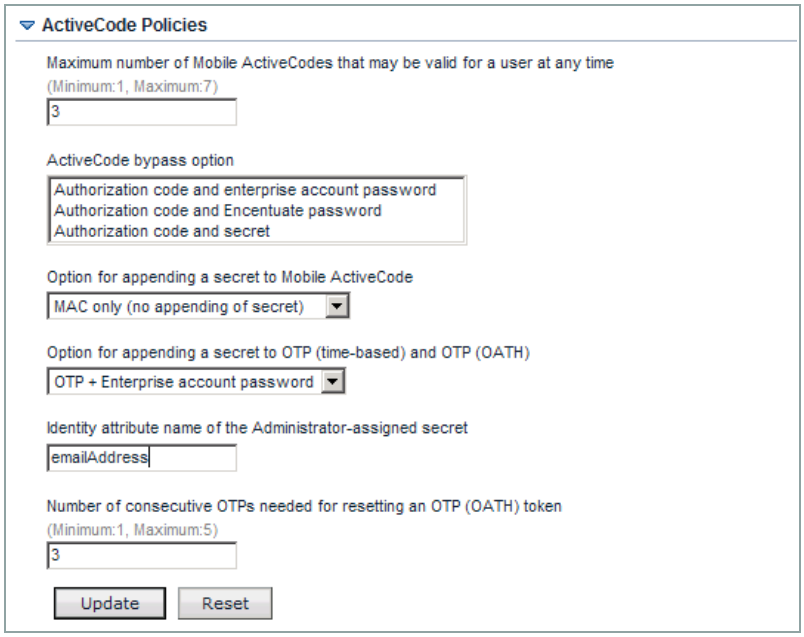
3. Under **Authentication Policies**, select the authentication mode(s) to be supported for the authentication service. In this case, **OTP**, **MAC** or both.

4. Click **Update**.

To modify ActiveCode system policies using AccessAdmin:

1. Click **System Policies** in the AccessAdmin navigation panel.

2. Click **ActiveCode Policies**. The ActiveCode Policies panel is displayed.



ActiveCode Policies panel

3. Specify the **Maximum number of Mobile ActiveCodes that may be valid for a user at any time**. For example, if a user should only be allowed to use the last MAC that was issued, this policy should be set to 1.

4. Set the **ActiveCode bypass option** to allow users to bypass ActiveCode authentication when they fail to obtain a MAC or OTP. Users can also use a combination of authorization code (issued by Helpdesk) and a known secret.

5. Set the **Option for appending a secret to Mobile ActiveCode**. If enabled, all MACs entered by users have to adhere to the specified format. Please note that the order is also specified in the policy values.

6. Set the **Option for appending a secret to OTP (time-based) and OTP (OATH)**. If enabled, all OTPs entered by users must adhere to the specified format. The order is also specified in the policy values.

7. Specify the **Identity attribute name of the Administrator-assigned secret** for appending to MAC or OTP.

8. Specify the **Number of consecutive OTPs needed for resetting an OTP (OATH) token**.

9. Click **Update**.

Enabling MAC for AccessAssistant and Web Workplace

To enable MAC for AccessAssistant and Web Workplace:

❶ Go to *Start >> Encentuate IMS Server >> AccessAdmin >> Authentication Service Policies*.

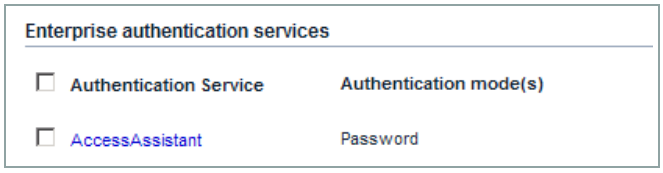
❷ Under **Personal Authentication Services**, mark the **AccessAssistant** check box.

Personal authentication services panel

❸ Click the **Move to enterprise authentication services** button to move AccessAgent in the **Enterprise Authentication Services** panel.

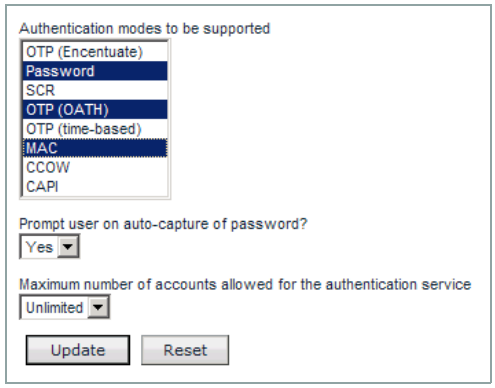
Click the Move to enterprise authentication services button

❹ In the **Enterprise Authentication Services** panel, click **AccessAssistant**. Scroll down to click **Authentication Policies**.



Click the AccessAssistant link

❺ In the **Authentication Policies** panel, select the **Authentication modes to be supported**. Hold down the **Ctrl** key and click to select multiple options. In this case, select **Password**, **OTP (OATH)**, and **MAC**.



Configure authentication policies and click Update

❻ Click **Update**.

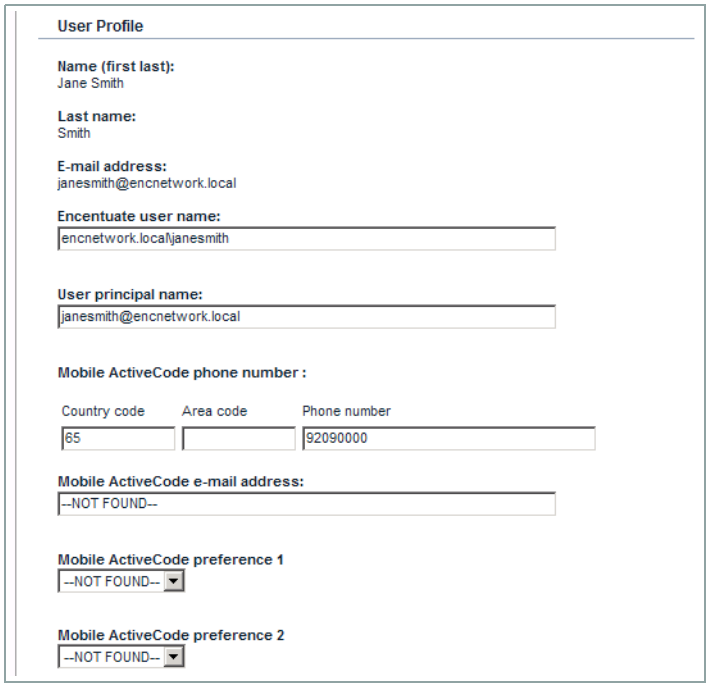
Enabling MAC for a user

Use AccessAdmin to enable MAC for a user. At least one MAC preference should be set, and the appropriate MAC-enabled authentication service must be enabled for the user.

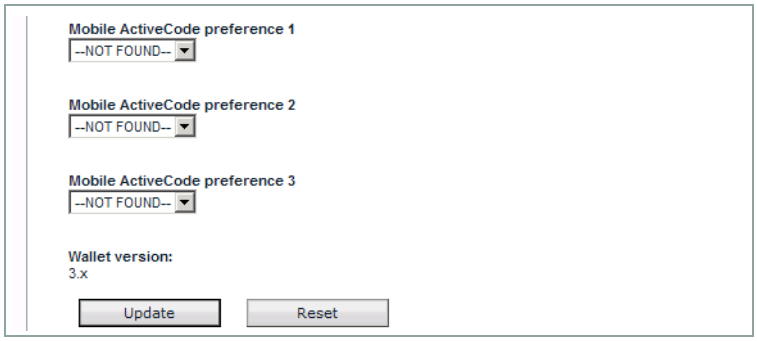
To enable MAC in AccessAdmin for a user:

❶ Click the user's name in the AccessAdmin navigation panel.

❷ In the **User Profile** panel, enter the MAC phone number and/or email address.



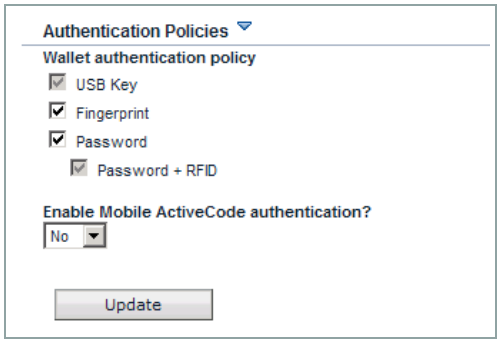
AccessAdmin User Profile panel (1/2)



AccessAdmin User Profile panel (2/2)

❸ Click **Update**.

❹ Scroll down to find the **Authentication Policies** panel and expand it.



AccessAdmin Authentication Policies panel

❺ Select **Yes** from the **Enable Mobile ActiveCode authentication?** drop-down list.

❻ Click **Update**.

Configuring RADIUS interface at the IMS Server

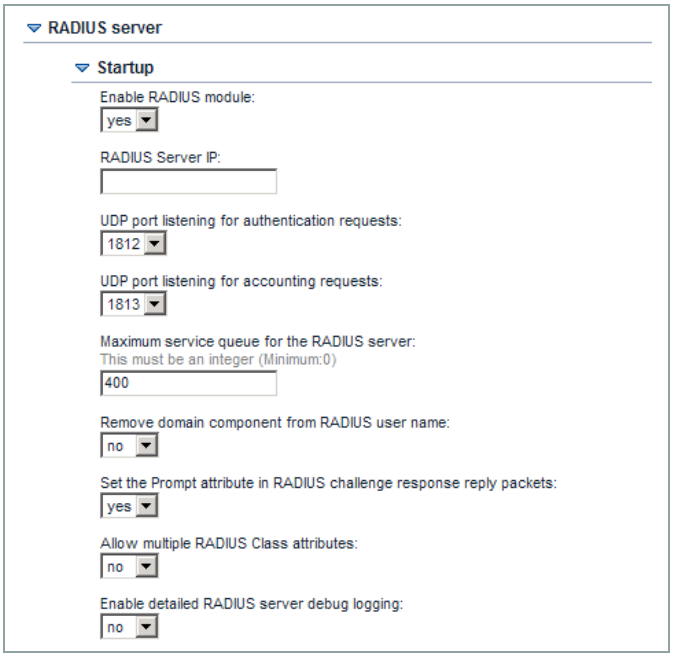
The RADIUS interface at the IMS Server can be configured using the Encentuate IMS Configuration Utility. Follow the steps below to configure the RADIUS interface.

This section covers the following topics:

Enabling RADIUS

To enable the RADIUS module:

❶ In the IMS Configuration Utility, expand the RADIUS Server panel (*Advanced Settings >> User Authentication >> RADIUS Server >> Startup*).



RADIUS Startup Configuration panel (1/2)

❷ From the **Enable RADIUS module** drop-down list, select **yes**.

❸ Enter the **RADIUS ServerIP**.

❹ Select the **UDP port listening for authentication requests** from the drop-down list. This is the port that the server listens to for RADIUS authentication requests.

❺ Select the **UDP port listening for accounting requests** from the drop-down list. This is the port that the server listens to for RADIUS accounting requests.

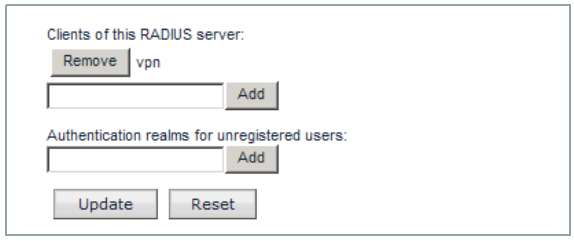
❻ Enter **400** as the **Maximum service queue for the RADIUS server**. Each authentication request generates one packet, so 400 is a reasonable figure.

❼ Select **no** from the **Remove domain component from RADIUS username** drop-down menu. This option strips the domain component from the username.

❽ Select **yes** from the **Set the Prompt attribute in RADIUS challenge response reply packets** dropdown menu. Some VPNs (notably checkpoint) will not allow RADIUS packets with the Prompt attribute set, while others (such as Aventail) require it to be set

❾ Select **no** from the **Allow multiple RADIUS Class attributes** dropdown menu. Enabling this will allow the user's LDAP attributes to be correctly sent as multiple RADIUS Class attributes. However, for VPNs that can handle only a single RADIUS Class attribute, this feature will have to be disabled.

❿ Select **no** from **Enable detailed RADIUS server debug logging** dropdown menu. Enable this option only when needed for troubleshooting and debugging because this affects performance and privacy.



RADIUS Startup Configuration panel (2/2)

⓫ In the **Clients of this RADIUS server** field, key in a RADIUS client name, IP address/FQDN and click **Add.**

⓬ In the **Authentication realms for unregistered users** field, indicate a realm that non IMS users are authenticated against. Then click **Add**. An LDAP type realm can be used to retrieve member of and other user attributes for registered IMS users if the VPN user ID and the LDAP user ID match.

⓭ Click **Update** to save the startup configuration.

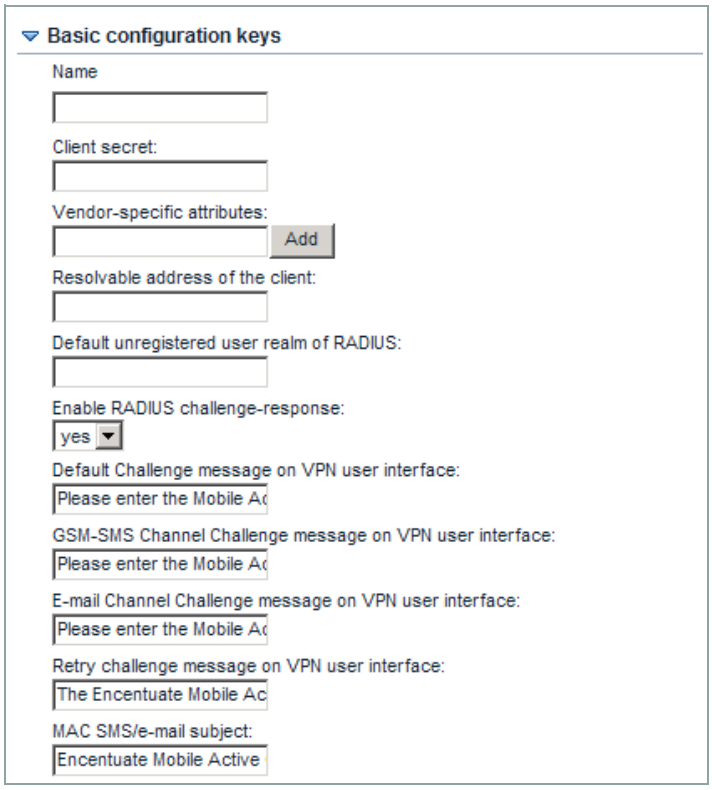
Adding a new RADIUS client configuration

Add a new RADIUS client configuration for every RADIUS client connecting to the IMS Server.

To add a RADIUS client configuration:

❶ Go to *Advanced Settings >> User Authentication >> RADIUS Server >> Add Configuration Group*.

❷ Select **RADIUS Client** from the drop-down list, then click **Configure**. The RADIUS client panel is displayed.



Add Configuration Group (1/2)

❸ In the **Basic Configuration Keys** panel, enter the **Name** of the new client.

❹ Enter a **Client secret**. This is the shared secret used to encrypt communication between the RADIUS server and client. This information is mandatory.

❺ Enter the **Resolvable address of the client**. This is the IP address or FQDN of the host listed as a RADIUS client. This information is mandatory

❻ Select **yes** for **Enable RADIUS challenge-response** to enable RADIUS challenge-response.

❼ Enter the **Default Challenge message on VPN user interface**. This is the default RADIUS challenge message that the user sees on the VPN user interface. This step is only required if MAC is enabled.

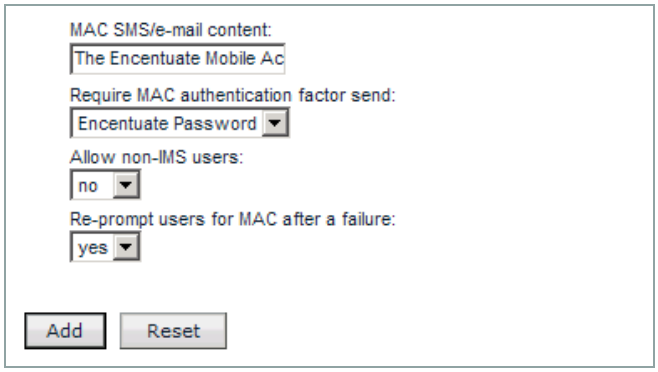
❽ Enter the **GSM-SMS Channel Challenge message on VPN user interface**. This is the RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent using an SMS gateway (such as, via a Web-based SMS message connector). This step is only required if MAC is enabled.

❾ Enter the **Email Channel Challenge message on VPN user interface**. This is the RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent using an email gateway (such as, via an Email message connector). This step is only required if MAC is enabled.

❿ Enter the **Retry challenge message on VPN user interface**. This is the RADIUS challenge message that the user sees on the VPN user interface when asked to retry following a failed verification attempt.

⓫ Enter the **Subject of MAC SMS or e-e-mail**. This is the template for the subject of the SMS or email message that the user will receive the MAC with. Use the placeholder "%MAC%" to indicate where the MAC should appear.

For example: If the text is "Your MAC is %MAC%", and the MAC is "5yd34t", the actual subject of the message will be "Your MAC is 5yd34t".



Add Configuration Group (2/2)

⓬ Enter the **MAC SMS/e-mail content**. This is the template for the body of the SMS or email message that the user will receive the MAC with. Use the placeholder "%MAC%" to indicate where the MAC should appear.

For example: If the text is "Your MAC is %MAC%", and the MAC is "5yd34t", the actual body of the message will be "Your MAC is 5yd34t".

⓭ Select **yes** to **Re-prompt users for MAC after a failure** if it is entered incorrectly. The user will be prompted until the account is locked.

⓮ Click **Add**. The *Startup Configuration >> Configured Keys* panel is redisplayed.

⓯ Restart the **IMS Server** for the changes to take effect.

Installing AccessAgent for Terminal Services or Citrix

Install AccessAgent on each Windows Terminal Server or Citrix, if used in the integrated remote access deployment.

Standard AccessAgent can be installed on the Citrix client. The installer automatically installs the Citrix related components and configures some Citrix settings, if the computer has Citrix client (such as, ICA client) installed.

However, the required components and settings will be gone under any of the following circumstances:

- ICA client is upgraded.
- ICA client is re-installed.
- ICA client is installed only after AccessAgent is installed.

To reinstate the required components and settings, execute the `ConfigureCitrixClientForAA.vbs` script in the Encentuate program files folder (**C:\Program Files\Encentuate**).

If AccessAgent 3.3.2.6 and above is uninstalled, and an earlier version of Access-Agent is subsequently installed (such as, downgrading to earlier version of Access-Agent), the changes made in Citrix's **module.ini** file would not be done correctly.

In such cases, edit the **module.ini** file manually.

To edit module.ini manually:

1. Edit the `module.ini` file (usually in **C:\Program Files\Citrix\ICA Client**) using a text editor.
2. Remove all lines that contain `TSVCClient.dll`.
3. Execute `ConfigureCitrixClientForAA.vbs` script in the Encentuate program files folder.

Installing AccessAgent on a MetaFrame server

Consider the following when installing AccessAgent on MetaFrame server:

- **Do you want to replace Citrix server's Gina with Encentuate Gina?**

  Do not replace Gina. The installer **SetupHlp.ini** file should be configured for this. That means when the user directly connects to a Citrix Server without local AccessAgent, the user will see MSGina's logon screen.

For AccessAgent 3.3.0.0 and above, the behavior of the **EnginaEnabled** *option in* **SetupHlp.ini** *is consistent for workstations, Terminal Servers, and Citrix servers. Select option* **0** *for Citrix servers.*

- **How do you install Encentuate Network Provider DLL and enable it?**

  The Network Provider DLL called EnNetworkProvider.dll captures the user's AD user name and password when logging on to the MetaFrame server. The AccessAgent uses the AD user name and password as the Encentuate user name and password for logging on to the user's Wallet. The entire logon process is seamless from the user's point of view

  An installer configuration is available in the file **SetupHlp.ini**.

  Set the flag **EncentuateNetworkProviderEnabled** to **1** before installation.

  Set the machine policy **pid_en_network_provider_enabled** (**EnNetworkProviderEnabled**) to **1**. This can be set by the installer by including it in the **DeploymentOptions.reg** file.

Embedding application links in an enterprise portal

Links to Web applications, Windows Terminal Servers, and Citrix servers, can be embedded in an enterprise portal. The succeeding topics will discuss instructions for embedding such links.

This section covers the following topics:

Web application

To embed each Web application in the enterprise portal, use the following format:

"https://WebWorkplaceHost/WebWorkplacePath/
link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true"

Where:

- **WebWorkplaceHost** is the hostname of the Web server hosting Web Workplace
- **WebWorkplacePath** is the relative path of Web Workplace on the Web server hosting it
- **authserviceid** is the authentication service ID to be used, and appid is the application ID of the application

Sample link:

https://ims.company.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true

Windows Terminal Server or Citrix server

To embed each Windows Terminal Server or Citrix server link in the enterprise portal, do the following to get the URL:

1. Create a graphical terminal shortcut in **Aventail WorkPlace** for the Windows Terminal Server or Citrix server.
2. Log on to **Aventail WorkPlace**.
3. Right-click on the graphical terminal shortcut and select **Properties**.
4. Copy the "Address (URL)". It should be of the form: "javascript:openWebifierURL('/workplace/access/exec/webifier?id=AV1167931536750AO&resourceType=host&path=rdp://citrix.company.com", 800, 600)

   To embed the URL in the enterprise portal, follow this format:

   "https://AventailWorkPlace/WorkPlaceLink"

   Where:

   - **AventailWorkPlace** is the hostname of the Aventail SSL VPN server
   - **WorkPlaceLink** is the relative path within quotes in the URL obtained in step 4 above.

   Sample link:

   https://vpn.company.com/workplace/access/exec/webifier?id=AV1167931536750AO&resourceType=host&path=rdp://citrix.company.com

Web Workplace portal page

To embed the Web Workplace portal page in the enterprise portal, follow this format:

https://WebWorkplaceHost/WebWorkplacePath/index_basic_auth.jsp

Where:

- WebWorkplaceHost is the hostname of the Web server hosting Web Workplace
- WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it.

Sample link:

https://ims.company.com/WebWorkplace/index_basic_auth.jsp

Integrating with Aventail SSL VPN

Aventail SSL VPN is one of the various VPN appliances supported by the IAM Remote Access Integration.

Configure the Aventail SSL VPN appliance to use the IMS Server as an authentication server, and launch applications from Web Workplace.

This section covers the following topics:

Configuring authentication servers

To configure authentication servers:

1. Log on to the Management Console of Aventail SSL VPN.
2. From the main navigation menu, click **Authentication Servers**. The **Authentication Servers** page is displayed.
3. Click **New...** to define a new authentication server.

❹ Select **RADIUS** as the authentication directory type, and click **Continue**.

❺ Enter a name for the authentication server.

❻ Enter the host name or IP address of the IMS Server as that of the **primary RADIUS server**. If the IMS Server is configured to listen on a port other than 1645 (the default), you can specify a port number as a colon-delimited suffix, for example, ims.company.com:1812.

❼ Enter the RADIUS client secret that you have specified in the IMS Server RADIUS configuration as the **shared secret** here.

❽ Click **Save** to store the configuration.

Configuring realms

To configure realms:

❶ From the main navigation menu, click **Realms**. The Realms page is displayed.

❷ Click **New** to define a new realm.

❸ Enter a name for the realm and select the IMS authentication server you have defined above as the authentication server.

❹ Click **Finish** to store the configuration.

Configuring services

To configure services:

❶ From the main navigation menu, click **Services**. The Services page is displayed.

❷ In the **Access services** area, click the Configure link for **Web proxy service**. The Configure Web Proxy Service page is displayed.

❸ Click the **Web Application Profiles** tab, and then click **New**. The Add/Edit Web Application Profile page is displayed.

❹ Enter a name for the Web Workplace profile (for example, "WWPAuth").

❺ Under the **Single Sign-On** section, choose **Forward each user's individual username and password**.

❻ Under the **Content translation** section, choose the following options: **Translate cookie body** and **Translate cookie path**.

Configuring resources

To configure resources:

1. From the main navigation menu, click **Resources**. The Resources page is displayed.
2. Under the **Resources** tab, click **New** and select **URL...**.
3. Enter a name for the resource (for example, "WWP").
4. Enter the **URL** of the Web Workplace hosting server (for example, https://ims.company.com).
5. Mark the **Create shortcut on Aventail WorkPlace** checkbox so that steps 1 to 4 in the **Configure Aventail WorkPlace** section below can be simplified.
6. Under the **Advanced Web resource options** section, give the resource an **Alias name** (for example, "wwp") and choose the **web application profile** created earlier (for example, "WWPAuth").
7. Click **Save** to store the configuration.

Configuring Aventail WorkPlace

To configure Aventail WorkPlace:

1. From the main navigation menu, click **Aventail WorkPlace**. The Aventail WorkPlace page is displayed.
2. In the **WorkPlace shortcuts** tab, click **New** and select **Web shortcut...**.
3. Give an appropriate **Number**, and **Link** text.
4. Choose the **Resource** configured earlier (for example, "WWP") and click **Next**.
5. For the **Start** page, provide the link relative to the URL given above.

   For the Web Workplace portal page, use the URL: "/WebWorkplacePath/index_basic_auth.jsp", where WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it.

   For each Web application to embed in the enterprise portal, use a URL of the form: "/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true"

   where: WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to use, and appid is the application ID of the application.

The following is an example link: "/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true".

6. Click **Finish** to store the configuration.
7. From the main navigation menu, click **Services**. The Services page is displayed.
8. Click the **Configure** link for Aventail WorkPlace in the *Access services* section. The Configure Workplace page is displayed.
9. Under **Web shortcut access**, select **Use Web content translation (provides single sign-on)**.
10. Click **Save** to store configuration.

Configuring Access Control

To configure Access Control:

1. From the main navigation menu, click **Access Control**. The Access Control page is displayed.
2. Ensure that the access control rules allow your users to access the resources defined above. For more information on access control configuration, see the IAM Administration Guide.

Configuring SSL settings

To configure SSL settings:

1. From the main navigation menu, click **SSL Settings**. The SSL Settings page is displayed.
2. Click the **Edit** link in the **CA certificates** section.
3. Click **New** to import the IMS Root CA certificate (and the Web Workplace site certificate, if they are different).
4. Choose **Certificate file** to import each certificate. To get the certificate of a Web site using Internet Explorer:

    1. Visit the Web site.
    2. Click **lock** to view certificates.
    3. Click the **Details** tab and **Copy to File...** to export the certificate as a .CER file, which can then be imported into the SSL VPN.

Completing the configuration

To complete the configuration:

1. Click **Pending changes** on the top right, and click **Apply Changes**.
2. On the next user logon to the Aventail SSL VPN, Web Workplace should be visible as a configured application. SSL VPN should be able to log on to Web Workplace automatically when clicked.

Integrating with Juniper SSL VPN

Configure the Juniper SSL VPN appliance to use the IMS Server as an authentication server, and to treat Web Workplace as a resource from which applications can be launched.

This section covers the following topics:

Configuring authentication servers

To configure authentication servers:

1. Log on to the **Central Manager** of the Juniper SSL VPN.
2. Click **Auth. Servers** from the main navigation menu. The Authentication Servers page is displayed.
3. Go to *(Select server type) >> Radius Server >> New Server…* to define a new authentication server.
4. Enter a name for the authentication server.

❺ Enter the host name or IP address of the IMS Server as that of the RADIUS Server. If the IMS Server is configured to listen on something other than 1645 (the standard), you can specify a port number in Authentication Port.

❻ Enter the RADIUS client secret that you have specified in the IMS Server RADIUS configuration as the Shared Secret here.

❼ Enter the IP address of the Juniper SSL VPN in **NAS-IP-Address** field.

❽ Mark the **Users authenticate using tokens or one-time passwords** checkbox.

❾ Under **Custom challenge expressions**, mark the **Generic Login** checkbox and enter **(.*)** in the corresponding text box.

❿ Click **Save Changes** to store the configuration.

Configuring user realms

To configure user realms:

❶ Click **User Realms** from the main navigation menu. The User Authentication Realms page is displayed.

❷ Click **New** to define a new realm.

❸ Enter a name for the realm and select the IMS authentication server you have defined above as the authentication server.

❹ Click **Save Changes** to store the configuration.

Configuring signing-in

To configure signing-in:

❶ Click **Signing In** from the main navigation menu. The Signing In page is displayed.

❷ Select the **Sign-in Pages** tab, and click the **Upload Custom Pages...** button.

❸ Click **Sample** to download a ZIP file containing sample sign-in pages from the Sample Template Files panel.

❹ Modify both **Defender.thtml** and **Defender-ppc.thtml** in the ZIP file as follows:

1. Delete the word: "Challenge: "

2. Delete the line: " Enter the challenge string above into your token, and then enter the one-time response in the field below. "

3. Replace the word "Response:" with "Mobile ActiveCode:".

❺ Rename the ZIP file as **sign-in_mac.zip**.

❻ Enter **Mobile ActiveCode Sign-In Page** as Name for the custom sign-in pages.

❼ Click **Browse...** and select the ZIP file **sign-in_mac.zip**.

❽ Click **Upload Custom Pages** to upload the custom sign-in pages.

❾ Select the **Sign-in Policies** tab.

❿ Under **User URLs**, click ***/** to configure user sign-in to use the newly-created custom sign-in pages.

⓫ Select **Mobile ActiveCode Sign-In Page** for **Sign-in page**.

⓬ Make sure that IMS is in the list of Selected realms under the **Authentication realm**.

⓭ Click **Save Changes** to store the configuration.

Configuring Web resources profiles

To configure Web resource profiles:

❶ Click **Resource Profiles** from the main navigation menu. The Resource Profiles page is displayed.

❷ Click *Web Applications/Pages >> New Profile...* to create a new Web resource.

❸ Give an appropriate name to the resource (e.g., Web Workplace).

❹ Give the Base URL of the Web Workplace hosting server (e.g., https://ims.company.com).

❺ Click **Show ALL autopolicy types >>** to configure advanced policies.

❻ Mark the **Autopolicy: Single Sign-on** checkbox and click the **Basic Auth** radio button.

❼ Click the **Use predefined credentials...** and **Variable Password:** radio buttons. Enter "<USER>" for Username and "<PASSWORD>" in the **Variable Password** field.

❽ Click **Save and Continue >** to store the configuration.

❾ Select appropriate Roles and click **Save Changes**.

❿ Select the **Bookmarks** tab and click the automatically created bookmark.

⓫ Enter "/WebWorkplace/index_basic_auth.jsp" in the URL field.

⓬ Click **Save Changes** to store the bookmark. This will be the bookmark for accessing Web Workplace.

⓭ Click **New Bookmark...** to create a bookmark for accessing a Web application through Web Workplace.

⓮ Enter a name for the Web application.

⓯ Use the following URL format:

"/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true"

where: WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application. The following is an example link:

"/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true".

⓰ Click **Save Changes** to store the bookmark.

Configuring terminal services resources

To configure terminal services resources:

❶ Click **Resource Profiles** from the main navigation menu. The Resource Profiles page is displayed.

❷ Click **Terminal Services** and then **New Profile...** to create a new Terminal Services resource.

❸ Give an appropriate name to the resource (e.g., "Terminal Server").

❹ Enter the host name or IP address of the terminal server as Host.

❺ Click **Save and Continue >** to store the configuration.

❻ Select appropriate **Roles** and click **Save Changes**.

❼ Select the **Bookmarks** tab and click the automatically created bookmark.

❽ Under **Authentication**, enter "<USER>" for Username and "<PASSWORD>" for **Variable Password**.

❾ Click **Save Changes** to store the bookmark. This will be the bookmark for accessing terminal services.

Configuring SSL settings

To configure SSL settings:

1. Click **Configuration** from the main navigation menu. The Configuration page is displayed.
2. Select the **Certificates** tab.
3. Click **Trusted Server CAs**.
4. Click **Import Trusted Server CA...** to import the IMS Root CA certificate (and the Web Workplace site certificate, if they are different).
5. Click **Browse...** to import the certificate. Visit the Web site, and click the **lock** icon to view certificates and get the certificate of a Web site using Internet Explorer. Select the **Details** tab and click **Copy to File...** to export the certificate as a .CER file, which can then be imported into the SSL VPN.
6. Click **Import Certificate** to complete the process.

Embedding application links in an enterprise portal

Links to Web applications, Windows Terminal Servers, and Citrix servers, can be embedded in an enterprise portal. The following are instructions for embedding such links:

Web application

For each Web application to embed in the enterprise portal, use a URL of the form:

https://WebWorkplaceHost/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application.

The following is an example link:

https://ims.company.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true

Windows Terminal Server or Citrix server

Refer to the Juniper Networks Secure Access Administration Guide for instructions on creating links from an external site to a terminal services session bookmark.

The following is an example link:

https://<IVE>/dana/term/winlaunchterm.cgi?bmname=<bookmarkName>

Web Workplace portal page

To embed the Web Workplace portal page in the enterprise portal, use a URL of the form:

https://WebWorkplaceHost/WebWorkplacePath/index_basic_auth.jsp

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; and WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it.

The following is an example link:

https://ims.company.com/WebWorkplace/index_basic_auth.jsp

Integrating with F5 SSL VPN

You need to configure the F5 SSL VPN appliance to use the IMS Server as a RADIUS authentication server for a user group, and to treat Web Workplace as a Web application resource.

This section covers the following topics:

Configuring user groups

To configure user group:

1. Log on to the Admin Console of the F5 SSL VPN.
2. In the navigation pane, click **Users**, expand **Groups**, and click **Master Groups**. The **Master Groups** screen is displayed.
3. Click the **Create new group** button.
4. Enter a name for the group (e.g., "IMS").

❺ Select **External** for users in group

❻ Select **RADIUS** for authentication method.

❼ Click **Create** to create the new group.

❽ Select the **Authentication** tab.

❾ Enter the host name or IP address of the IMS Server in the **Server** field. If the IMS Server is configured to listen on something other than 1645 (the standard), you can specify a port number in Port.

❿ Enter the RADIUS client secret that you have specified in the IMS Server RADIUS configuration as the **Shared Secret**. Enter the same thing in **Confirm Shared Secret**.

⓫ Click **Save Settings** to store the configuration.

⓬ Select the **Resource Groups** tab.

⓭ Click an available resource group (e.g., Default_resource) and click the **Add >** button to assign resources.

⓮ Click **Update** to store the configuration.

⓯ Click **Global Settings** in the navigation pane. The **Global Settings** screen appears

⓰ Mark the **Use extra domain password for single sign on** checkbox and click **Update** to store the configuration.

Customize WebDAV

To customize WebDAV:

The FirePass user logon page should be customized not show the extra domain password field since it is supposed to be the same as the user's Encentuate password.

❶ Create an **HTTP** Web Service on the Device Management : Configuration : Network Configuration : Web Services screen to enable WebDAV-based customization.

❷ Select the **Allow insecure access** option on the Device Management : Security : User Access Security screen.

❸ Mark the **Allow WebDAV sandbox customization** checkbox on the Device Management : Customization screen and enter a WebDAV password in the text box that is displayed.

❹ The WebDAV sandbox is accessed via HTTP at the URI /**sandbox** as the user **webdav**. For example, if the FirePass controller has been configured using the steps above with an HTTP web service at 192.168.0.99, use the URL http://192.168.0.99/sandbox/.

❺ Go to the FirePass user logon page and save it as **index.htm**.

❻ Modify **index.htm** as follows:

1. Delete the domain password label and input field:

```
<tr valign=top>

<td><img src="images/my/tr.gif" width="16" height="1"
alt="alt="" border="0"></td>

<td align=left><span class=o>Domain password<br>(use cached if
empty):</span><br></td>

</tr>

<tr valign=top>

<td><img src="images/my/tr.gif" width="16" height="1"
alt="alt="" border="0"></td>

<td align=left><input type=password class=lp_input size="13"
name="dpassword" autocomplete="off"><br></td>

</tr>
```

2. Insert this script right after the deleted domain password label and input field:

```
<INPUT type="hidden" name="dpassword">

<SCRIPT LANGUAGE='VBScript'>

sub Setdpassword()

  e1.dpassword.Value = e1.password.Value

end sub

</SCRIPT>
```

3. Change the **onclick** property of the logon button by replacing the line:

```
<input name=login id=submitform type=submit class=o
value="Logon">

with:

<input name=login id=submitform onclick='Setdpassword()'
type=submit class=o value="Logon">
```

❼ Upload **index.htm** to FirePass using WebDAV.

1. Launch **My Network Places** in Windows.
2. Click **Add a network place**.
3. Click **Next** twice,
4. Enter the URL stated in step 4 above,
5. Log on using webdav as user name and the WebDAV password as password.
6. Drag and drop the **index.htm** file into the explorer window.

Configuring Web application resources

To configure Web application resources:

❶ Click **Portal Access** in the navigation pane. Expand **Web Applications** and click **Resources**. The Resources screen is displayed.

❷ Click **Add New Favorite** to create a favorite for accessing a Web application through Web Workplace.

❸ Enter a name for the Web application.

❹ Use a URL of the form:

"https://WebWorkplaceServer/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true"

where: WebWorkplaceServer is the server hosting Web Workplace; WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application. The following is an example link:

"https://wwp.encentuate.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true".

❺ Mark the **Open in new window** checkbox.

❻ Click **Add New** to store the favorite.

❼ Include the appropriate URLs in the **Allow list** under **Access Control Lists.**

❽ Click **Master Group Settings** in the navigation pane. The Master Group Settings screen is displayed.

❾ Select the **Master Group** that you created earlier (e.g., IMS).

❿ Under **NTLM and Basic Auth Proxy**, mark the checkboxes for **Proxy Basic and NTLM auth using FirePass user logon form**, and **Auto-logon to Basic and NTLM auth protected sites using FirePass user credentials**. Then select **Basic Authentication** as the Preference.

Configuring terminal server resources

To configure terminal server resources:

❶ Click **Application Access** in the navigation pane. Expand **Terminal Servers**, and click **Resources**. The Resources screen is displayed.

❷ Click **Add New Favorite** to create a favorite for accessing a Terminal Server.

❸ Enter a name for the Terminal Server.

❹ Enter the host name or IP address of the Terminal Server in the **Host** field.

❺ Select **Microsoft Terminal Server** for Port.

❻ Click **Add New** to store the favorite.

❼ Click **Master Group Settings** in the navigation pane. The Master Group Settings screen is displayed.

❽ Select the **Master Group** that you created earlier (e.g., IMS).

❾ Mark the **Auto-logon to applicable Terminal Servers using FirePass user logon credentials** checkbox under **Screen resolution**.

Embedding application links in enterprise portals

Links to Web applications, Windows Terminal Servers, and Citrix servers, can be embedded in an enterprise portal. The following are instructions for embedding such links:

Web application

For each Web application to be embedded in the enterprise portal, use a URL of the form:

"https://WebWorkplaceHost/WebWorkplacePath/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true"

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it; authserviceid is the authentication service ID to be used, and appid is the application ID of the application.

The following is a sample link:

https://ims.company.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true

Windows Terminal Server or Citrix server

To obtain a direct link to the FirePass Terminal Server client, you can log on to FirePass, launch your Terminal Server favorite, and copy the URL that shows up in the URL field of the browser.

The following is a sample link:

https://<FirePass>/vdesk/index.php3?Z=0,7

Web Workplace portal page

To embed the Web Workplace portal page in the enterprise portal, use a URL of the form:

https://WebWorkplaceHost/WebWorkplacePath/index_basic_auth.jsp

where: WebWorkplaceHost is the hostname of the Web server hosting Web Workplace; and WebWorkplacePath is the relative path of Web Workplace on the Web server hosting it.

The following is an example link:

https://ims.company.com/WebWorkplace/index_basic_auth.jsp